ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(НИУ «БелГУ»)

ИНСТИТУТ УПРАВЛЕНИЯ

КАФЕДРА СОЦИАЛЬНЫХ ТЕХНОЛОГИЙ

ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ (НА МАТЕРИАЛАХ БЕЛГОРОДСКОЙ ТАМОЖНИ)

Дипломная работа студента
обучающегося по специальности 38.05.02 «Таможенное дело»
очной формы обучения группы 05001304
Живилова Дмитрия Вячеславовича

Научный руководитель
канд. социол. наук,
доцент Гайдукова Г.Н.

Рецензент
начальник информационно-технической службы Белгородской таможни, капитан таможенной службы
Сорокин Д.С.

БЕЛГОРОД 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования.Эффективное обеспечение национальной безопасности России является основой спокойной жизни российских граждан, реализации ими конституционных прав, функционирования государственной власти и, в целом, процветания общества. Неотъемлемой частью национальной безопасности выступает информационная безопасность. Возрастание роли информации, информационных технологий и ресурсов актуализирует вопросы информационной безопасности в системе обеспечения национальной безопасности государства, общества и личности. Эти вопросы напрямую касаются и таможенных органов как основного института государства, обеспечивающего его национальную безопасность в экономической сфере.

Вопросы практического обеспечения информационной безопасности таможенных органов нашли отражения в Концепции обеспечения информационной безопасности таможенных органов РФ на период до 2020 года[1]. Однако, вопросы теоретической проработки и анализа практического обеспечения информационной безопасности таможенных органов с организационно-правовой точки зрения в должной мере не нашли отражения трудах ученых.

Особое место в системе обеспечения информационной безопасности таможенных органов занимает организационное регулирование, заключающееся в разработке принципов, методов, средств и мер по ее обеспечению. Это обосновывает необходимость проведения теоретических исследований по обеспечению информационной безопасности таможенных органов с организационно-правовых позиций, раскрывая роль и значимость данной деятельности, полноту ее правовой регламентации и разработки рекомендаций по повышению эффективности практической работы.

---

[1]Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года : Приказ ФТС России от 13 декабря 2010 года № 2401. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

Анализ степени изученности темы. Вопросы обеспечения информационной безопасности органов государственной власти как основа современного государственного управления исследовались в работах Л.Н. Алексеевой, А.Е. Ведерникова, Л.И. Купрюхиной, Л.Ю. Медовкиной, К.С. Растрыгиной, А.В. Русанова, П.Ю. Филяк, П.С. Шубина[1] и др.

Вопросы межведомственного информационного взаимодействия и применения информационных технологий в практике таможенного управления исследовались Е.Г. Бормотовой, В.В. Гарбуз, Л.Д. Зайцевой, Е.В. Зыбиной, Э.П. Куприновым, С.В. Курихиным, С.А. Куштапина, Н.Г. Липатовой, В.В. Саенко, Ю.И. Сомовым, Ю.В. Тарарышкина, В.В. Черных, А.В. Ускова, О.В. Ясенева[2] и др.

---

[1]Алексеева Л.Н. Система информационной безопасности органов государственной власти как основа современного государственного управления // Вестник Университета (Государственный университет управления). 2015. № 13; Ведерников А.Е. Актуальные проблемы обеспечения информационной безопасности в органах государственного управления : сб. «Актуальные вопросы обеспечения информационной безопасности». Белгород, 2015; Купрюхина Л.И. Культура информационной безопасности в органах государственной власти // Инновации в гражданской авиации. 2016. № 1; Медовкина Л.Ю. Эффективность деятельности государственных органов в сфере обеспечения информационной безопасности : материалы II Международной научно-практической конференции «Государственная политика: методология, практика, направления совершенствования» / Под редакцией П.А. Меркулова. Орел, 2017; Растрыгина К.С. Совершенствование системы информационной безопасности в органах государственной власти : сб. статей IX международной научно-практической конференции «EurasiaScience». М., 2017; Филяк П.Ю., Русанов А. В. Обеспечение информационной безопасности в органах государственной власти на основе качественного подхода к анализу рисков : сб. международной научно-практической конференции «Современные проблемы и задачи обеспечения информационной безопасности (СИБ - 2015)». М., 2015; Шубин П.С. Информационная безопасность органов государственной власти: сб. статей международной научно-практической конференции: в 3 частях «Информация как двигатель научного прогресса». Екатеринбург, 2017.

[2]Бормотова Е.Г., Липатова Н. Г. Межведомственное информационное взаимодействие для обеспечения выполнения контрольных функций таможенными органами: монография. М., 2014; Саенко В.В., Куштапин С. А. , Гарбуз В. В. , Черных В. В. , Зыбина Е. В. Основные направления развития информационно-коммуникационных технологий в таможенных органах Российской Федерации // Транспортное дело России. 2015. № 3; Сомов Ю.И., Купринов Э.П., Курихин С.В., Зайцева Л.Д. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов: монография. М., 2014; Тарарышкин Ю.В. Информационные технологии – инструмент управления внешнеторговыми операциями : материалы IV Международной научно-практической конференции «Информационные технологии в экономике, бизнесе и управлении». Тамбов, 2017; Усков, А.В., Ясенев О. В. Информационные таможенные технологии. Нижний Новгород, 2014.

Отдельные аспекты обеспечения информационной безопасности таможенных органов рассматривались в трудах:Г.И. Барбышевой и Ш.Ф. Мирзаева, П.Н. Башлы, Е.В. Бурьковой и А.В. Масловой, Г.Ю. Власенкова и В.А. Карданова, С.Н. Клименко, В.И. Кореньковой, Е.Ю. Крайдуба, И.В. Мильшиной и А.О. Медведевой, Н.А. Мошкиной, Б.Г. Никитина, П.Н. Хлыстовой, А.А. Чеботаревой, С.А. Шавшиной и П.А. Нуратиновой[1] и др.

[1]Барбышева Г.И., Мирзаев Ш. Ф. Обеспечение информационной безопасности таможенных органов РФ : материалы II Международной научной конференции «Инновационная экономика». Казань, 2015; Башлы П.Н. Актуальные проблемы информационной безопасности в таможенных органах Российской Федерации : материалы научно-практической конференции: в 2 частях «Особенности государственного регулирования внешнеторговой деятельности в современных условиях». Р-на-Д, 2015; Бурькова Е.В., Маслова А. В. Задача обеспечения информационной безопасности таможенных органов : материалы XI Всероссийской научно-практической конференции «Современные информационные технологии в науке, образовании и практике». Оренбург, 2014; Власенков Г.Ю., Карданов В. А. Информационная безопасность таможенных технологий: монография. М., 2016; Клименко С.Н. Правовые основы информационной безопасности в таможенных органах Российской Федерации : монография. СПб., 2013; Кожуханов Н.М. Направления обеспечения информационной безопасности таможенных органов : материалы VI Международной молодежной научно-практической конференции «Основные направления развития таможенного дела в условиях членства России во всемирной торговой организации». М., 2014; Коренькова В.И. Обеспечение информационной безопасности: таможенный аспект // Ростовский научный журнал. 2017. № 1; Крайдуба Е.Ю. Проблемы обеспечения информационной безопасности в таможенных органах Российской Федерации: сб. статей международной научно-практической конференции в 3-х частях «Научные революции: сущность и роль в развитии науки и техники». Уфа, 2017; Мильшина И.В., Медведева А. О. Информационное обеспечение деятельности таможенных органов: вопросы безопасности // Информационная безопасность регионов. 2013. № 1 (12); Мошкина Н.А. Обеспечение информационной безопасности таможенных органов на современном этапе : материалы III всероссийской научно-практической конференции: в 2 частях «Особенности государственного регулирования внешнеторговой деятельности в современных условиях». Р-на-Д, 2016; Никитин Б.Г. Информационная безопасность таможенных органов Российской Федерации в контексте интеграционных процессов // Академический вестник Ростовского филиала Российской таможенной академии. 2016. № 2 (23); Хлыстова П.Н. Совершенствование методов обеспечения информационной безопасности в таможенном деле : сб. научных статей V Всероссийской междисциплинарной молодежной научной конференции «Проблемы правовой и технической защиты информации сборник». Барнаул, 2017; Чеботарева А.А. К вопросу о проблемах обеспечения информационной безопасности в таможенных органах // Таможенное дело. 2012. № 2; Шавшина С.А., Нуратинова П. А. Применение информационных технологий в таможенной сфере и анализ проблем информационной безопасности : сб. трудов конференции «Тенденции инновационных процессов в науке». М., 2015.

Проблема исследования заключается в сложившемся противоречии между необходимостью повышения эффективности обеспечения информационной безопасности таможенных органов и недостаточной теоретической обоснованностью организационного механизма решения данной задачи.

Объектом дипломного исследованияявляется система обеспечения информационной безопасности таможенных органов.

В качестве **предмета исследования** выступает механизм обеспечения информационной безопасности Белгородской таможни.

Цель исследования – разработка рекомендаций по повышению эффективности обеспечения информационной безопасности таможенных органов.

Задачи исследования:

–изучить теоретические основ организации системы обеспечения информационной безопасности таможенных органов;

– рассмотреть нормативно-правовые основы организации системы обеспечения информационной безопасности таможенных органов;

– проанализировать практику обеспечения информационной безопасности Белгородской таможни;

– предложить направления совершенствования обеспечения информационной безопасности таможенных органов.

Теоретико-методологические основы исследования. Теоретическую базу исследования составили разработанные учеными положения в области теории безопасности, права, а также труды отечественных исследователей в сфере обеспечения информационной безопасности (А.В. Морозов, Т.А. Полякова)[1], а также механизма обеспечения информационной

[1]Морозов А.В., Полякова Т. А. Организационно-правовое обеспечение информационной безопасности : монография. М., 2013.

безопасности таможенных органов (А.М. Воронов, Н.М. Кожуханов, Е.С. Недосекова)[1]

В качестве методологической основы дипломной работы использовались диалектический метод и основанная на нем система общенаучных и частных научных методов (при изложении материала дипломного исследования); анализ (в процессе выработки научных определений понятий «информационная безопасность», «обеспечение информационной безопасности таможенных органов»); синтез (при обобщении полученных теоретических результатов, формулировке выводов по главам); системный анализ (при изучении механизмов организационного регулирования обеспечения информационной безопасности таможенных органов); сравнительно-правовой метод (при выявлении особенностей административной деятельности таможенных органов в исследуемой сфере); системный метод (при раскрытии целостности объекта исследования) и другие методы.

Эмпирическая база исследования:

– Таможенный кодекс ЕАЭС[2];

–федеральное законодательство, нормативно-правовые акты Федеральной таможенной службы РФ в сфере информационной безопасности таможенных органов[3];

---

[1]Воронов А.М., Кожуханов Н. М. Содержание правового института «информационная безопасность таможенной деятельности» // Финансы: теория и практика. 2013. № 4 (76); Кожуханов Н.М. Модель обеспечения информационной безопасности таможенной деятельности: монография. М., 2012; Недосекова Е.С. Административно-правовой механизм обеспечения информационной безопасности таможенных органов Российской Федерации: монография. М., 2013.

[2]Таможенный кодекс Евразийского экономического союза (приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза) // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

[3]О таможенном регулировании в Российской Федерации : федер. закон от 27 ноября 2010 года № 311-ФЗ (ред. от 28.12.2017) // Собр. законодательства Рос. Федерации. – 2010. - № 48. – Ст. 6252; О Стратегии развития таможенной службы Российской Федерации до 2020 года : Распоряжение правительства РФ от 28 декабря 2012 года № 2575-р // Собр. законодательства Рос. Федерации. – 2013. – № 2. – Ст. 109; Об утверждении положения и состава совета по обеспечению информационной безопасности таможенных органов Российской Федерации : Приказ ФТС Росси от 22 августа 2011 года № 1702 // Справочно-

–статистическая отчетность Белгородской таможни.

Научно-практическая значимость исследования определяется выводами и рекомендациями прикладного характера, которые могут быть использованы в целях совершенствования регулирования объекта исследования, сделанными на основе оценки организационно-правового регулирования обеспечения информационной безопасности таможенных органов, изучения практики его применения.

Структура дипломной работы представлена введением, двумя главами, заключением и списком источников и литературы.

правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОРГАНИЗАЦИИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ

1.1. Сущность и содержание организации системы обеспечения информационной безопасности таможенных органов

На современном этапе развития таможенные органы обеспечивают реализацию внешнеторговых интересов государства, противодействуют угрозам безопасности России, пополняют доходную часть федерального бюджета.

Инновационный характер стратегического вектора развития РФ способствует формированию благоприятных перспектив эффективной интеграции страны в мировое хозяйство, развитию внешнеэкономической деятельности, разработке стратегии развития таможенной службы на долгосрочную перспективу. Одним из направлений Стратегии развития таможенной службы РФ до 2020 года выступают задачи развития информационно-технического обеспечения таможенной деятельности в области повышения уровня защищенности информационных ресурсов.

Сегодня, быстрые темпы развития информационно-коммуникационных технологий, ставших основой таможенных процессов, значительный рост «информационных ресурсов, информационных систем и специфических информационных технологий, увеличивающиеся объемы статистики внешней торговли, и персональных данных лиц, перемещающих товары, доступ к коммерческой тайне участников внешнеэкономической деятельности в процессе применения таможенных операций»[1] требуют постоянного совершенствования системы обеспечения информационной безопасности.

---

[1]Барбышева Г.И., Мирзаев Ш.Ф. Обеспечение информационной безопасности таможенных органов РФ : материалы II Междунар. науч. конф. «Инновационная экономика». URL :https://moluch.ru/conf/econ/archive/170/8659/ (дата обращения: 10.03.2018).

В целях дальнейшего исследования остановимся на характеристике понятий «безопасность», «угрозы», «информация», «информационная безопасность».

Общетеоретическое понятие «безопасность» определяется как «отсутствие опасности»[1], «состояние, при котором не угрожает опасность, есть защита от опасности»[2]. При этом, опасность рассматривается как «возможность, угрозу чего-нибудь опасного, т.е. способного причинить какой-нибудь вред, несчастье»[3]. В свою очередь, угроза представляет собой «возможную опасность, запугивание, обещание причинить кому-нибудь неприятность, зло»[4]. Следовательно, безопасность можно трактовать как отсутствие угрозы для чего-нибудь, либо кого-нибудь. Близко к данному определению раскрывается понятие безопасности в справочной литературе ««ситуация, при которой кому- или чему-нибудь не существует угрозы со стороны кого- или чего-либо, при этом не исключается наличие одновременно нескольких источников опасности. Безопасность потенциальных жертв обеспечивается, когда конкретные жертвы парируют все существующие опасности либо когда опасностей для них не существует»[5].

Под информацией мы будем понимать «сведения, являющиеся объектом хранения, передачи и преобразования»[6].

В целом, под информационной безопасностью понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество

---

[1]Даль В. Толковый словарь живого великорусского языка. М., 1989. С. 67.
[2]Ожегов С.И. Словарь русского языка. М., 1990. С. 67.
[3]Там же.
[4]Ожегов С.И. Указ. Соч. С. 716
[5]Безопасность России: Правовые, социально-экономические и научно-технические аспекты: словарь терминов и определений / науч. рук. К.В. Фролов. М., 1999. С. 56.
[6]Барбышева Г.И., Мирзаев Ш.Ф. Обеспечение информационной безопасности таможенных органов РФ : материалы II международной научной конференции «Инновационная экономика». URL: https://moluch.ru/conf/econ/archive/170/8659/ (дата обращения: 10.03.2018).

и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[1].

«Обеспечение информационной безопасности призвано решать основные задачи: выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам; защита прав юридических и физических лиц на интеллектуальную собственность, а также сбор, накопление и использование информации; защита государственной, служебной, коммерческой, личной и других видов тайн»[2].

Следует отметить, что «роль информационной безопасности и ее место в системе национальной безопасности страны определяются тем, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, где последняя выступает важным связующим звеном всех основных компонентов государственной политики в единое целое»[3].

Таможенная служба в Российской Федерации выступает частью системы обеспечения информационной безопасности, защищая экономические интересы страны и обеспечивая эффективное вхождение российской экономики в международное экономическое пространство. В этих условиях обеспечение информационной безопасности становится одним из основных видов деятельности таможенных органов.

---

[1]Доктрина информационной безопасности Российской Федерации : Указ Президента РФ от 05 декабря 2016 года № 646. URL: http://www.garant.ru/products/ipo/prime/doc/71456224/#ixzz5CESMZNGw (дата обращения: 06.03.2018).

[2]Барбышева Г.И., Мирзаев Ш.Ф. Обеспечение информационной безопасности таможенных органов РФ :материалы II международной научной конференции «Инновационная экономика». URL: https://moluch.ru/conf/econ/archive/170/8659/ (дата обращения: 10.03.2018).

[3]Недосекова Е.С. Цели и принципы обеспечения информационной безопасности таможенных органов. URL: http://www.justicemaker.ru/view-article.php?art=3059&id=25 (дата обращения: 06.03.2018).

В соответствии с Доктриной информационной безопасности РФ по своей общей направленности в части таможенных органов Российской Федерации угрозы информационной безопасности подразделяются на следующие виды:

– угрозы конституционным правам и свободам человека и гражданина в информационной сфере деятельности таможенных органов РФ;

– угрозы информационному обеспечению государственной политики в области таможенного дела;

– угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей таможенных органов РФ в ее продукции, а также обеспечению накопления, сохранности и эффективного использования также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов в области таможенного дела;

– угрозы обеспечению безопасности информации в автоматизированных информационных системах таможенных органов РФ.

В положении «Стратегии развития таможенной службы Российской Федерации до 2020 года в разделе 8 «Совершенствование информационно-технического обеспечения» установлено, что «повышение уровня защищенности информационных ресурсов, расширение спектра мер по обеспечению информационной безопасности, в том числе при организации защищенного обмена информацией с федеральными органами исполнительной власти – это одна из основных задач, решение которой будет содействовать совершенствованию информационно-технического обеспечения деятельности таможенных органов»[1].

Следовательно, обеспечение информационной безопасности – этонасущная необходимость и одно из приоритетных направлений обеспечения безопасности таможенных органов, реализующих функции по

[1]О Стратегии развития таможенной службы Российской Федерации до 2020 года : Распоряжение Правительства РФ от 28 декабря 2012 года № 2575-р (ред. от 10 февраля 2018 года) // Собр. законодательства Рос. Федерации. – 2013. – № 2. – Ст. 109.

защите экономических интересов Российской Федерации. Ведь таможенные органы располагают значительными информационными ресурсами, информационными системами и специфическими информационными технологиями, ведут статистику внешней торговли, получают и используют при осуществлении таможенного контроля персональные данные лиц, перемещающих товары, имеют доступ к коммерческой тайне участников внешнеэкономической деятельности в процессе применения таможенных операций.

Согласно Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года под информационной безопасностью таможенных органов понимается «стояние защищенности национальных интересов государства в информационной сфере деятельности таможенных органов РФ»[1]. Целью обеспечения информационной безопасности таможенных органов РФ выступает «защита этих интересов при осуществлении ФТС России функций по выработке государственной политики и нормативному правовому регулированию, контролю и надзору в области таможенного дела, а также функции агента валютного контроля и специальных функций по борьбе с контрабандой, иными преступлениями и административными правонарушениями»[2].

С целью дальнейшей характеристики механизма обеспечения информационной безопасности таможенных органов, следует отметить, что безопасность информации распадается на две составляющие: безопасность содержательной части и защищенность информации от внешнего воздействия, вплоть до уничтожения. В связи с чем, в организации обеспечения информационной безопасности в таможенных органах можно выделить несколько направлений работы:

– защита данных, передаваемых между таможенными органами;

---

[1]О Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года : Приказ ФТС России от 13 декабря 2010 года № 2401 // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

[2] Там же.

– защита информации, обрабатываемой в автоматизированных системах;

– защита информации при использовании электронной цифровой подписи и электронного документооборота;

– защита информации при несанкционированном доступе;

– обеспечение безопасности при организации международного информационного обмена.

Осуществление любой деятельности основывается на четко сформулированных и систематизированных принципах. Проведя анализ нормативно правовых актов РФ и ФТС России, научных работ монографического характера, в части вопросов, касающихся информационной безопасности, представляется возможным выделить две группы принципов: принципы информационной безопасности и принципы организации обеспечения информационной безопасности.

К первой группе принципов можно отнести: законности, гласности, свободы поиска, гуманизма и другие.

«Вторая группа принципов должна лежать в основе построения системы информационной безопасности для того, чтобы с ее помощью оптимально достигались поставленные цели и задачи. В эту группу отнесем такие принципы, как оптимальная организация системы; системность; комплексность; приоритет предупредительных мер в целях обеспечения информационной безопасности; сочетание гласных и негласных методов и средств обеспечения информационной безопасности; простота и гибкость системы; научно-техническая обоснованность и использование опыта и др.»[1].

При этом, основываясь на теории права, все принципы можно классифицировать на: общеправовые, отраслевые и специальные.

«К общеправовым принципам можно отнести принципы верховенства права, законности, гуманизма, приоритета, уважения, соблюдения и защиты

[1]Недосекова Е.С. Цели и принципы обеспечения информационной безопасности таможенных органов. URL : http://www.justicemaker.ru/view-article.php?art=3059&id=25 (дата обращения: 06.03.2018).

прав и свобод человека и гражданина и т.д. Отраслевыми принципами являются те, которые характерны для всей информационной сферы и распространяются на все информационные отношения. Остальные из рассматриваемых принципов относятся к специальным, т.к. они характеризуют именно процессы обеспечения информационной безопасности и построения системы информационной безопасности таможенных органов. Такая систематизация принципов поможет в организации работы по эффективному обеспечению информационной безопасности таможенных органов»[1].

Организация деятельности таможенных органов по обеспечению информационной безопасности осуществляется в рамках сформированного организационно-правового механизма, который представляет собой совокупность субъектов и объектов воздействия, способов, методов, мер и мероприятий, обеспечивающих состояние защищенности объектов, информации, ее свойств, инфраструктуры и т.д.

Проводя анализ объектов обеспечения информационной безопасности можно выделить следующие сферы, сгруппированные по сферам жизнедеятельности государства и общества.

Первая – сфера внутренней политики государства. В рамках данной сферы объектами выступают:

«а) конституционные права и свободы человека и гражданина, являющегося должностным лицом или работником таможенных органов Российской Федерации;

б) персональные данные физических лиц – субъектов персональных данных;

в) специальная категория персональных данных (состояние здоровья) должностных лиц, работников и пенсионеров таможенных органов Российской Федерации, членов их семей при использовании

[1]Недосекова Е.С. Цели и принципы обеспечения информационной безопасности таможенных органов. URL: http://www.justicemaker.ru/view-article.php?art=3059&id=25 (дата обращения: 06.03.2018).

информационных систем в лечебно-санаторных учреждениях ФТС России. Речь идёт о Центральной поликлинике ФТС России, Центральном клиническом госпитале ФТС России и т.п.;

г) открытые информационные ресурсы таможенных органов Российской Федерации»[1].

Вторая – сфера внешней политики России, в рамках которой объектами будут выступать информационные ресурсы представительств таможенной службы России за рубежом, посредством которых организуется трансграничный обмен информацией.

Третья – сфера экономики России. В рамках данной сферы объектами выступают:

- информация, получаемая таможенными органами России в соответствии с таможенным законодательством ЕАЭС и Российской Федерации, иными нормативными правовыми актами РФ, составляющая государственную, коммерческую, банковскую, налоговую тайну и другую конфиденциальную информацию;

- документы и сведения, используемые в статистических целях;

- права правообладателей на объекты интеллектуальной собственности.

Четвертая – правоохранительная и судебная сферы. Объектами в них выступают информационные ресурсы подразделений, реализующих правоохранительные функции, содержащие специальные сведения и оперативные данные служебного характера.

Пятая – сфера общегосударственных информационных и телекоммуникационных систем. Объектами данной сферы выступают:

«а) объекты информатизации таможенных органов Российской Федерации, предназначенные для обработки сведений, отнесённых к государственной тайне. В категорию объектов информатизации законодатель

[1]Кожуханов Н.М. Специфика правового регулирования информационной безопасности таможенных органов : сб. материалов международной научно-практической конференции «Единое окно», обмен данными, межведомственное и государственно-частное сотрудничество при упрощении процедур торговли. М., 2011. С. 128.

также включает средства вычислительной техники, информационно-вычислительные комплексы, средства звукозаписи и звукоусиления, звукосопровождения, переговорные и телевизионные устройства, средства тиражирования документов, сети и системы, операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение, автоматизированные системы управления, системы связи и передачи данных, осуществляющие приём, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

б) технические средства и системы, обрабатывающие открытую информацию, но размещённые в помещениях, в которых обрабатывается информация ограниченного доступа;

в) помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа;

г) автоматизированные информационные системы таможенных органов Российской Федерации, включая ведомственную интегрированную телекоммуникационную сеть и локальные вычислительные сети таможенных органов Российской Федерации, а также средства вычислительной техники и программного обеспечения»[1].

Шестая сфера – это область науки и техники. Объектами безопасности здесь выступают:

«а) результаты проведённых по заказу таможенных органов Российской Федерации фундаментальных, поисковых и прикладных научных исследований, потенциально важных для научно-технического, технологического и социально-экономического развития страны, включая

[1]Кожуханов Н.М. Специфика правового регулирования информационной безопасности таможенных органов : сб. материалов международной научно-практической конференции «Единое окно», обмен данными, межведомственное и государственно-частное сотрудничество при упрощении процедур торговли. М., 2011. С. 129.

сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

б) открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование, разработанные или полученные в интересах таможенных органов Российской Федерации;

в) научно-технические кадры таможенных органов Российской Федерации»[1].

Основными субъектами воздействия будут являться специально созданные и обладающие полномочиями в данной области подразделения таможенных органов.

В рамках реализации Концепции создан Совет по обеспечению информационной безопасности таможенных органов РФ, являющийся «постоянно действующим внештатным органом ФТС России по проведению государственной политики в области обеспечения информационной безопасности, в том числе защиты сведений, составляющих государственную тайну, в таможенных органах Российской Федерации и в учреждениях, находящихся в ведении ФТС России. Совет выполняет функции ведомственной постоянно действующей технической комиссии ФТС России по защите государственной тайны»[2].

К основным задачам Совета относятся:

«а) обеспечение надежного и эффективного управления системой защиты государственной тайны и ее функционирования в таможенных органах;

---

[1]Кожуханов Н.М. Специфика правового регулирования информационной безопасности таможенных органов : сб. материалов международной научно-практической конференции «Единое окно», обмен данными, межведомственное и государственно-частное сотрудничество при упрощении процедур торговли. М., 2011. С. 129.

[2]Об утверждении Положения и состава Совета по обеспечению информационной безопасности таможенных органов Российской Федерации : Приказ ФТС России от 22 августа 2011 года № 1702. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=95940861001615614130202103 2&cacheid=AE20AA55A28A5B324D79E0E3350E0D8A&mode=splus&base=EXP&n=649587&rnd=94C670460BBB10D2A45FA5D49BA781BC#0711783940898455 (дата обращения: 03.03.2018).

б) организация и координация работ по противодействию иностранным техническим разведкам и по технической защите информации;

в) рассмотрение программ создания и совершенствования системы информационной безопасности таможенных органов;

г) выработка единой технической политики в области защиты информации в Единой автоматизированной информационной системе таможенных органов;

д) совершенствование системы физической и технической защиты объектов таможенных органов»[1].

Также «оказывают воздействие специальные органы обеспечения информационной безопасности, к которым следует отнести Федеральное агентство по печати и массовым коммуникациям, Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (находятся в ведении Министерства связи и массовых коммуникаций Российской Федерации); ФСБ России, МВД России, Совет Безопасности РФ, а также другие структуры, в чью компетенцию входит обеспечение информационной безопасности РФ»[2].

Следующим элементом механизма является его содержательная часть, т.е. то, как, с помощью каких средств, в каких целях, каким образом оказывается административно-правовое воздействие. Основными формами воздействия будут являться:

– действия, направленные – на превентивное воздействие;

– непосредственное регулирование (регламентация);

– установление запрета вплоть до привлечения к ответственности.

---

[1]Об утверждении Положения и состава Совета по обеспечению информационной безопасности таможенных органов Российской Федерации : Приказ ФТС России от 22 августа 2011 года № 1702. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=95940861001615614130202103 2&cacheid=AE20AA55A28A5B324D79E0E3350E0D8A&mode=splus&base=EXP&n=649587&rnd=94C670460BBB10D2A45FA5D49BA781BC#0711783940898455 (дата обращения: 03.03.2018).

[2]Недосекова Е.С. Цели и принципы обеспечения информационной безопасности таможенных органов России. URL: http://www.justicemaker.ru/view-article.php?art=3059&id=25 (дата обращения: 21.03.2018).

Таким образом, обеспечение информационной безопасности таможенных органов – многоаспектная деятельность, состоящая в создании условий, при которых нанесение вреда зависящим от информации элементам системы (свойствам, законным интересам, инфраструктуре или порядку функционирования субъектов информационных отношений и др.) в сфере деятельности таможенных органов становится невозможным или крайне затруднительным. Среди таких условий имеются основания для выделения следующих:

– соблюдение принципов информационной безопасности и построения системы обеспечения информационной безопасности;

– разработка и поддержание в таможенных органах соответствующего административно-правового режима, обеспечивающего защиту от несанкционированного доступа к информации;

– выработка действенного механизма административного воздействия на поведение должностных лиц таможенных органов и третьих лиц в целях обеспечения информационной безопасности таможенных органов РФ;

– разработка конкретных и реальных мер и мероприятий по обеспечению информационной безопасности таможенных органов;

– разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности таможенных органов, как на федеральном, так и на ведомственном уровне;

– проведение своевременного, периодического, выборочного, планового и внепланового контроля за соблюдением данного режима и выполнением предусмотренных мероприятий и другие условия.

Следует сказать, что за нарушение правовых норм, регулирующих информационную безопасность таможенных органов, положены различные виды ответственности: дисциплинарная, гражданско-правовая, административная, уголовная. Это обусловлено спецификой совершаемого правонарушения. Соответственно, применяемые меры ответственности носят

достаточно широкий спектр, начиная от выговора, административного штрафа и оканчивая лишением свободы.

1.2. Нормативно-правовые основы организации системы обеспечения информационной безопасности таможенных органов

Обеспечение информационной безопасности в таможенных органах организуется в соответствии с Указом Президента РФ № 646 «Об утверждении доктрины информационной безопасности Российской Федерации»[1], которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В целом, законодательство в сфере информационной безопасности таможенных органов условно можно разделить на две группы.

В первую группу нормативных правовых актов, определяющую меры, направленные на соблюдение конституционных прав и свобод субъектов правоотношений в информационной сфере, развитие современных информационных и телекоммуникационных технологий, а также установление правил участия Российской Федерации в международном информационном обмене, включены Конституция РФ[2], законы «О государственной тайне»[3], «О безопасности»[4], «О стратегическом планировании»[5], «О связи»[1], «Об информации, информационных

---

[1]Об утверждении Доктрины информационной безопасности Российской Федерации : Указ президента РФ от 05 декабря 2016 года № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.

[2]Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 21 июля 2014 года № 11-ФКЗ) // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.

[3]О государственной тайне : Закон РФ от 21 июля 1993 года № 5485-1 (ред. от 26 июля 2017 года) // Собр. законодательства Рос. Федерации. -1997. – № 41. – Ст. 8220-8235.

[4]О безопасности : федер. закон от 28 декабря 2010 года № 390-ФЗ (ред. от 05 октября 2015 года) // Собр. законодательства Рос. Федерации. – 2011. – № 1. – Ст. 2.

[5]О стратегическом планировании в Российской Федерации : федер. закон от 28 июня 2014 года № 172-ФЗ (ред. от 31 декабря 2017 года) // Собр. законодательства Рос. Федерации. – 2014. – № 26 (часть 1). – Ст. 3378.

технологиях и о защите информации»[2], «О персональных данных»[3], «О коммерческой тайне»[4].

Важную роль в административно-правовом регулировании отношений в области информационной безопасности играют также Таможенный кодекс ЕАЭС[5], законы «О таможенном регулировании»[6], «О государственной гражданской службе»[7] и многие другие.

Каждый из перечисленных правовых актов в той или иной степени регулирует правовые отношения, направленные на достижение целей обеспечения информационной безопасности, образуя основу для формирования целостной системы информационной безопасности.

Вторая группа нормативных правовых актов, которую составляют Уголовный кодекс Российской Федерации (УК РФ)[8], Кодекс Российской Федерации об административных правонарушениях[9], а также ведомственные нормативные правовые акты (в том числе правовые акты по обеспечению информационной безопасности таможенных органов), закрепляет меры предупредительно-карательного характера.

---

[1]О связи : федер. закон от 07 июля 2003 года № 126-ФЗ (ред. от 05 декабря 2017 года) // Собр. законодательства Рос. Федерации.– 2003. – №28. – Ст. 2895.

[2]Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 года № 149-ФЗ (ред. от 25 ноября 2017 года) // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3448.

[3]О персональных данных : федер. закон от 27 июля 2006 года № 152-ФЗ (ред. от 29 июля 2017 года) // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3451.

[4]О коммерческой тайне : федер. закон от 29 июля 2004 года № 98-ФЗ (ред. от 12 марта 2014 года) // Собр. законодательства Рос. Федерации. – 2004. – № 32. – Ст. 3283.

[5]Таможенный кодекс Евразийского экономического союза (приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза). URL: http://www.eaeunion.org/ (дата обращения: 12.02.2018).

[6]О таможенном регулировании в Российской Федерации : федер. закон от 27 ноября 2010 года № 311-ФЗ (ред. от 29 декабря 2017 года) // Собр. законодательства Рос. Федерации. – 2010. – № 48. – Ст. 6252.

[7]О государственной гражданской службе Российской Федерации : федер. закон от 27 июля 2004 года № 79-ФЗ (ред. от 28 декабря 2017 года) // Собр. законодательства Рос. Федерации. – 2004. – № 31. – Ст. 3215.

[8]Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (ред. от 19 февраля 2018 года) // Собр. законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.

[9]Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ (ред. от 07 марта 2018 года) // Собр. законодательства Рос. Федерации. – 2002. – № 1 (Ч. 1). – Ст. 1.

Отдельно остановимся на нормативных правовых актах ФТС России, направленных на обеспечение информационной безопасности таможенных органов. Данные подзаконные акты конкретизируют специфику правового регулирования в рамках правового режима обеспечения информационной безопасности таможенных органов.

Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года, утвержденная приказом ФТС России №2401 от 13 декабря 2010 года[1]. Данный нормативный правовой акт раскрывает роль и место обеспечения информационной безопасности таможенных органов Российской Федерации в обеспечении национальных интересов государства в информационной сфере посредством формулировки определения, что считать информационной безопасностью таможенных органов, освещения составляющих национальных интересов Российской Федерации в информационной сфере деятельности таможенных органов, обозначения объектов обеспечения информационной безопасности таможенных органов.

В концепции описывается современное состояние информационной безопасности таможенных органов Российской Федерации, раскрывается политика и основные принципы обеспечения информационной безопасности таможенных органов. Данный документ выделяет основные направления и задачи обеспечения информационной безопасности таможенных органов на период до 2020 года. Отдельный раздел концепции посвящён организации контроля за состоянием обеспечения информационной безопасности таможенных органов.

Концепция служит методологической основой для:

– проведения единой политики обеспечения информационной безопасности таможенных органов РФ;

[1]Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года : Приказ ФТС России от 13 декабря 2010 года № 2401. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

– совершенствования правовых актов ФТС России, регламентирующей обеспечение информационной безопасности таможенных органов РФ;

– совершенствования организационно-режимных и технических мероприятий и методов обеспечения информационной безопасности таможенных органов РФ;

– разработки планов по дооснащению таможенных органов РФ сертифицированными по требованиям безопасности информации средствами информатизации (средствами вычислительной техники, программным обеспечением, средствами защиты информации и т.д.), а также по их внедрению и эксплуатации в повседневной деятельности таможенных органов РФ;

– подготовки предложений по совершенствованию ведомственной системы обеспечения информационной безопасности таможенных органов РФ.

Концепция выделяет четыре составляющих национальных интересов РФ в информационной сфере:

1) соблюдение конституционных прав и свобод человека и гражданина в области получения и использования таможенной информации, а также информации о сведениях и доказательствах, полученных в ходе оперативно-розыскной деятельности, уголовного и административного судопроизводства;

2) информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ с обеспечением доступа граждан к открытым государственным информационным ресурсам в таможенной сфере;

3) содействие развитию современных информационных технологий отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой

рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов, находящихся в ведении ФТС России;

4) защита информационных ресурсов таможенных органов РФ от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых в интересах таможенных органов РФ[1].

Положение по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации[2], которое «определяет условия и единый порядок использования в структурных подразделениях ФТС России, таможенных органах Российской Федерации, организациях, находящихся в ведении ФТС России, информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети Интернет»[3]. В соответствии с данным Положением, среди основных целей применение сети Интернет в таможенных органах выделяют:

«–обеспечение свободного доступа к информации о деятельности Федеральной таможенной службы с применением информационных технологий;

–размещение таможенными органами достоверной и своевременно обновленной информации о своей деятельности в сети Интернет;

---

[1]Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года : Приказ ФТС России от 13 декабря 2010 года № 2401. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

[2]Об утверждении Положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации : Приказ ФТС РФ от 07 октября 2010 года № 1866 // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

[3]Там же.

–поиск и получение общедоступной информации из сети Интернет;

–размещение заказов на поставки товаров, выполнение работ, оказание услуг в интересах таможенных органов;

–создание условий для предварительного информирования о товарах и транспортных средствах, декларирования товаров путем заявления таможенному органу в таможенной декларации в электронной форме сведений о товарах, о таможенном режиме и других сведений, необходимых для таможенных целей;

–получение общедоступной информации по направлению деятельности структурных подразделений с целью оперативного решения вопросов»[1].

К основным угрозам безопасности информации при использовании сети Интернет таможенными органами относятся:

«– заражение информационно-вычислительных ресурсов таможенных органов программными вирусами;

– несанкционированный доступ внешних пользователей к информационно-вычислительным ресурсам таможенных органов (в т.ч. целенаправленные сетевые атаки);

– внедрение в автоматизированные информационные системы таможенных органов программных закладок;

– загрузка трафика нежелательной корреспонденцией (спамом);

– несанкционированная передача информации ограниченного доступа должностными лицами таможенных органов в сеть Интернет;

– блокировка межсетевого взаимодействия с сетью Интернет путем нарушения целостности данных о настройках коммуникационного оборудования, обеспечивающего взаимодействие с сетью Интернет;

[1]Об утверждении Положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации : Приказ ФТС РФ от 07 октября 2010 года № 1866 // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

– нарушение целостности и достоверности открытых и общедоступных информационных ресурсов таможенных органов, размещаемых в сети Интернет»[1].

Положение о Совете по обеспечению информационной безопасности таможенных органов Российской Федерации[2], которое раскрывает назначение, цели и задачи, стоящие перед данным органом, раскрывает его структурные особенности и т.п.

Исходя из особенностей информации как объекта правового регулирования и анализа исследованных правовых актов, основополагающими принципами правового регулирования общественных отношений в информационной сфере являются законность, свобода информации, ограничение создания и распространения отдельных видов информации, защита информации[3].

Названные принципы закрепляют определенные механизмы регулирования правоотношений в сфере информационной безопасности таможенных органов, элементами которого, как известно, выступают нормы права, юридические факты, влекущие возникновение, изменение или прекращение правоотношений в обозначенной области, собственно правоотношения, реализацию прав, а также юридическую ответственность за правонарушение.

Государственная политика Российской Федерации в сфере обеспечения информационной безопасности реализуется через правотворчество,

---

[1]Об утверждении Положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации : Приказ ФТС РФ от 07 октября 2010 года № 1866 // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

[2]Об утверждении Положения и состава Совета по обеспечению информационной безопасности таможенных органов Российской Федерации : Приказ ФТС России от 22 августа 2011 года № 1702 // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

[3]Клименко С.Н. Информационная безопасность таможенных органов: актуальные направления совершенствования административно-правового обеспечения // Ученые записки Санкт- Петербургского имени В.Б. Бобкова филиала Российской таможенной академии. 2016. № 3 (59). С. 45.

правоприменение и участие государства в развитии правосознания и правовой культуры граждан. Развитие правотворчества и правоприменения в области обеспечения информационной безопасности Федеральной таможенной службы осуществляется в соответствии с основными задачами по обеспечению информационной безопасности, установленными Концепцией обеспечения информационной безопасности, ввиду существующих факторов, снижающих эффективность принимаемых мер.

Анализ действующих норм законодательства в области обеспечения информационной безопасности позволяет выделить три значимые области, включающие направления, подлежащие административному регулированию.

Первая область содержит три направления, из них первое направление заключается в соблюдении основных прав всех субъектов правоотношений в сфере получения и использования информации, обрабатываемой в таможенных органах, закрепленных в Конституции РФ. Данное направление необходимо учитывать для решения следующих задач:

– обеспечение конституционных прав и свобод субъектов правоотношений на свободный поиск и получение информации о действующих правовых актах в области таможенного дела;

– обеспечение доступа граждан и (или) организаций к достоверной информации в таможенных органах, необходимой для реализации их прав, свобод и обеспечения законных интересов;

– защиту информации ограниченного доступа, в том числе персональных данных должностных лиц и работников таможенных органов;

– защиту прав правообладателей на объекты интеллектуальной собственности при совершении таможенных операций.

Второе направление представляет собой информационное обеспечение государственной политики Российской Федерации. Данное направление связано с доведением до общественности достоверной информации и официальной позиции в области таможенного дела, в том числе опубликованием в официальных изданиях правовых актов ФТС России, а

также актов таможенного законодательства и иных правовых актов РФ в области таможенного дела; формированием общедоступных информационных ресурсов таможенных органов и повышением эффективности их использования.

Третье направление отражает развитие современных информационных таможенных технологий, обеспечение накопления, сохранности и эффективного использования информационных ресурсов таможенных органов и предусматривает решение следующих задач:

– опубликование в официальных изданиях актов таможенного законодательства Таможенного союза, иных правовых актов Российской Федерации в области таможенного дела и правовых актов ФТС России;

– формирование общедоступных государственных информационных ресурсов ФТС России и повышение эффективности их развития.

Вторая область – совершенствование ведомственной системы обеспечения информационной безопасности таможенных органов с учетом устойчивого роста количества нарушителей и угроз со стороны глобального информационного пространства в целом подразумевает:

– совершенствование нормативно-правовой базы обеспечения информационной безопасности таможенных органов с учётом современных динамично изменяющихся угроз и на основе анализа возможных рисков;

– совершенствование организационно-штатной структуры подразделений таможенных органов, отвечающих за обеспечение информационной безопасности и технической защиты информации, а также защиты государственной тайны;

– внедрение и развитие образовательных программ в области информационного права для всех категорий обучения, создание и совершенствование системы подготовки кадров в этой области;

– обучение должностных лиц структурных подразделений таможенных органов по вопросам обеспечения информационной безопасности таможенных органов;

– материально-финансовое обеспечение информационной безопасности таможенных органов.

Третья область – защита информационных систем таможенных органов от несанкционированного доступа, обеспечение безопасности информации, циркулирующей в Единой автоматизированной информационной системе таможенных органов (ЕАИС). В этом направлении должны выполняться следующие задачи:

– обеспечение различных административно-правовых режимов информации ограниченного доступа, обеспечение таможенных органов специальными видами связи, обеспечение безопасности информации на критически важных объектах таможенных органов, противодействие иностранным техническим разведкам;

– совершенствование механизмов электронной подписи в практике деятельности таможенных органов (создание, внедрение и развитие системы ведомственных удостоверяющих центров таможенных органов и инфраструктуры сертификатов открытых ключей пользователей автоматизированных информационных систем таможенных органов);

– обеспечение информационной безопасности таможенных органов при международном и межведомственном информационном обмене и информационном взаимодействии с участниками внешнеэкономической деятельности.

Таким образом, рассмотрев теоретические основы организации системы обеспечения информационной безопасности таможенных органов, можно сделать следующие выводы.

1. Информационная безопасность таможенных органов представляет собой состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная

целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

2. Обеспечение информационной безопасности призвано решать основные задачи: выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам; защита прав юридических и физических лиц на интеллектуальную собственность, а также сбор, накопление и использование информации; защита государственной, служебной, коммерческой, личной и других видов тайн

3. Организация деятельности таможенных органов по обеспечению информационной безопасности осуществляется в рамках сформированного организационно-правового механизма, который представляет собой совокупность субъектов и объектов воздействия, способов, методов, мер и мероприятий, обеспечивающих состояние защищенности объектов, информации, ее свойств, инфраструктуры и т.д. Законодательство в сфере информационной безопасности таможенных органов условно можно разделить на две группы. В первую группу нормативных правовых актов, определяющую меры, направленные на соблюдение конституционных прав и свобод субъектов правоотношений в информационной сфере, развитие современных информационных и телекоммуникационных технологий, а также установление правил участия Российской Федерации в международном информационном обмене. Вторая группа представлена нормативными правовыми актами, которые закрепляют меры предупредительно-карательного характера.

4. Правовому режиму информационной безопасности таможенных органов присущ императивный метод правового регулирования. Он предполагает использование властных предписаний абсолютно определенного характера, которые исходят от компетентного вышестоящего государственного органа или должностного лица (ФТС России) и обеспечиваются мерами принудительного характера.

ГЛАВА 2. ПРАКТИКА ОРГАНИЗАЦИИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЛГОРОДСКОЙ ТАМОЖНИ

2.1. Анализ организации системы обеспечения информационной безопасности Белгородской таможни

Белгородская таможня сегодня представляет собой одну из крупнейших в Центральном регионе России. «Белгородская таможня в числе лидеров по внедрению новых перспективных технологий таможенного контроля и таможенного оформления. Она одна из первых среди таможен ЦФО внедрила, а затем и перешла на 100% электронное декларирование с использованием электронной подписи, успешно применяет технологии удаленного выпуска в части хранения декларируемых товаров и предварительного информирования». Так по итогам 1 квартала 2018 года Белгородской таможней оформлено «9 380 деклараций на товары, 100% с применением электронной формы декларирования. Объем декларационного массива составляет 99,32 % от объема декларирования аналогичного периода 2017 года»[1].

Общая динамика оформленных деклараций по Белгородской таможне представлена в таблице 1.

Таблица 1

Объемы декларирования Белгородской таможней

показатели	годы			
	2014	2015	2016	2017
оформлено деклараций, всего	56749	45144	41678	42545
из них:				
на ввоз	11756	12901	13934	14040
на вывоз	44993	32243	27744	28505

Технологии электронного декларирования, удаленного выпуска, предварительного информирования используют информационный обмен в

[1] Основные итоги деятельности Белгородской таможни за 1 квартал 2018 года. Сайт ФТС России. URL: http://ctu.customs.ru/index.php?option=com_content&view=article&id=17016:-1-2018-&catid=103:info-o-tek-deyat-bel-cat&Itemid=145 (дата обращения: 19.04.2018).

режиме реального времени. «Это стало возможным благодаря повышению технической оснащенности таможни, а именно вычислительный комплекс таможни составляет компьютеров – 1252 единиц, серверов – 111 единиц, периферийных устройств (печатающие устройства, сканеры, МФУ) – 729 единиц, действующих автоматических телефонных станций 16 единиц, организовано и сопровождается 47 цифровых каналов передачи данных, объединяющих в телекоммуникационную вычислительную сеть все объекты Белгородской таможни. Для хранения, обработки и распределения доступа в таможне осуществляется администрирование 118 баз данных и 52 вида программных средств, предназначенных для проведения таможенных операций»[1].

Белгородской таможне «непосредственно подчинено 11 таможенных постов, 8 автомобильных, 7 железнодорожных пунктов пропуска и воздушный пункт пропуска – аэропорт международного значения Белгород. Из 8 автомобильных пунктов пропуска, функционирующих в регионе деятельности Белгородской таможни, 4 являются многосторонними – Грайворон, Ровеньки, Шебекино, Нехотеевка. Многосторонний автомобильный пункт пропуска Нехотеевка расположен на одной из важнейших автомагистралей, соединяющих центральную часть России с Республикой Крым и является крупнейшим автомобильным пунктом пропуска в Европе»[2]. Так же в подчинении таможни «находятся 3 отдела таможенного оформления и таможенного контроля с самостоятельным кодом в составе таможенных постов. В структуру таможни также входят 2 службы, 39 отделов и отделений, врачебный здравпункт и 4 отдельные должности. Околотаможенную инфраструктуру составляют 3 таможенно-логистических терминала (Грайворонский, Нехотеевский и Шебекинский), 24 склада

[1]Белгородская таможня подводит итоги. Сайт ФТС России. URL: http://ctu.customs.ru/index.php?option=com_content&view=article&id=16113:2017-12-22-06-09-57&catid=103:info-o-tek-deyat-bel-cat&Itemid=145 (дата обращения: 19.04.2018).

[2]Общая информация о Белгородской таможне. Сайт ФТС России. URL: http://ctu.customs.ru/index.php?option=com_content&view=article&id=433:obsch-inf-bel&catid=85:info-o-tam-org-bel-cat&Itemid=127 (дата обращения: 19.04.2018).

временного хранения, 2 таможенных склада, 5 магазинов беспошлинной торговли»[1].

С начала 2017 года «в Белгородской таможне оформление экспортно-импортных поставок осуществляли 1214 участников внешнеэкономической деятельности. Вывозом товаров из региона занимались 458 участников, ввозом – 954»[2].

С 2015 года на всех постах таможни реализована и успешно применяется технология автоматической регистрации электронных деклараций на товары.

«На всех постах Белгородской таможни осуществляется применение алгоритма автоматической регистрации и выпуска экспортных деклараций, автоматической регистрации деклараций на товары, поданных в форме электронного документа в соответствии с таможенной процедурой выпуска для внутреннего потребления. С июня 2016 года Белгородская таможня подключена к эксперименту по электронному взаимодействию с участниками ВЭД при помещении товаров под таможенную процедуру таможенного транзита. Сегодня большинство этапов взаимодействия участников ВЭД с таможенными органами осуществляются исключительно в электронном виде, начиная с предварительного информирования за несколько часов до ввоза товаров на таможенную территорию, помещения товаров на временное хранение, заканчивая подачей таможенной декларацией и выпуском товаров в соответствии с заявленной процедурой»[3].

В регионе деятельности таможни растет число участников внешнеэкономической деятельности, которые применяют удаленную форму уплаты таможенных платежей с использованием микропроцессорных пластиковых карт. В Белгородской таможне удаленная уплата таможенных платежей осуществляется на Белгородском, Валуйском и

---

[1]Белгородская таможня подводит итоги. Сайт ФТС России. URL: http://ctu.customs.ru/index.php?option=com_content&view=article&id=16113:2017-12-22-06-09-57&catid=103:info-o-tek-deyat-bel-cat&Itemid=145 (дата обращения: 19.04.2018).
[2]Там же.
[3]Там же.

Старооскольскомтаможенных постах операторами таможенных платежей. По итогам первого квартала 2018 года «в федеральный бюджет перечислено 5,2 млрд. руб.»[1]. а по итогам 2017 года «почти 23 млрд.рублей»[2].

Наряду с основным таможенным оформлением, обеспечение информационной безопасности является основным видом деятельности таможенных органов. «В настоящее время в Белгородской таможне используется Единая автоматизированная информационная система таможенных органов (ЕАИС ТО), которая создана с целью автоматизации работы таможенных органов Российской Федерации и реализации возложенных на ФТС России функций и полномочий в области таможенного дела:

– предоставление государственных услуг, а также функций и задач, обеспечивающих деятельность ФТС России;

– автоматизация деятельности должностных лиц и работников таможенных органов;

– формирование, ведение, резервирование и хранение информационных ресурсов таможенных органов;

– формирование и получение информации, содержащейся в информационных ресурсах таможенных органов»[3].

ЕАИС включает в себя 88 информационно-программных средств. Основными элементами ЕАИС являются локальные вычислительные сети (ЛВС), совокупность компьютерных баз данных, программные комплексы и объединяющая их ведомственная интегрированная телекоммуникационная сеть (ВИТС). ЕАИС ФТС России является распределенной

[1]Основные итоги деятельности Белгородской таможни за 1 квартал 2018 года. Сайт ФТС России. URL: http://ctu.customs.ru/index.php?option=com_content&view=article&id=17016:-1-2018-&catid=103:info-o-tek-deyat-bel-cat&Itemid=145 (дата обращения: 19.04.2018).

[2]Белгородская таможня подводит итоги. Сайт ФТС России. URL: http://ctu.customs.ru/index.php?option=com_content&view=article&id=16113:2017-12-22-06-09-57&catid=103:info-o-tek-deyat-bel-cat&Itemid=145 (дата обращения: 19.04.2018).

[3]Сведения о государственных информационных системах, находящихся в ведении Белгородской таможни. Сайт ФТС России. URL: http://ctu.customs.ru/index.php?option=com_content&view=article&id=437:sved-o-gos-inf-sis-bel&catid=121:info-o-gos-bel-cat&Itemid=163 (дата обращения: 25.04.2018).

автоматизированной информационной системой и охватывает всю территорию Российской Федерации, включая в себя Центральное информационно-техническое таможенное управление (ЦИТТУ), семь региональных вычислительных центров и транспортную подсистему ВИТС.

Белгородская таможня имеет собственную информационно-вычислительную сеть. Для информационного взаимодействия с участниками ВЭД, государственными и коммерческими структурами, информационными таможенными системами других государств ЕАИС ТО включает в свой состав автоматизированную систему внешнего доступа (АСВД) и систему ведомственных удостоверяющих центров таможенных органов на базе программного комплекса «КриптоПро УЦ».

Среди инструментов таможенного администрирования с применением информационных технологий, используемых на Белгородской таможне можно отметить:

– использование ИТ-технологий при совершении таможенных операций (электронное декларирование с использованием международной ассоциации «Интернет» (ЭД 2));

– программное использование системы управления рисками;

– электронный документооборот, позволяющий осуществлять информационный обмен данными;

– внедрение электронной подписи.

Белгородская таможня работает в рамках действия следующих информационных систем:

– КПС Портал ЭПС – комплекс программных средств портала электронного представления сведений;

– КПС Статистическое декларирование – комплекс программных средств, обеспечивающих прием и регистрацию статистических данных;

– КПС «Портал ЭД» – комплекс программных средств портала электронного представления сведений для электронного декларирования через Интернет

– КПС WEB-сервер ФТС России – комплекс программных средств WEB-сервера ФТС России;

– КПС «Декларант ЭДТиТС» – комплекс программных средств электронного декларирования товаров и транспортных средств.

Информационная безопасность и обеспечение защиты информации в Белгородской таможне реализована комплексом мероприятий, сущностью которых является обеспечение конфиденциальности, целостности и доступности информации. Для обеспечения защиты информации, передаваемой между таможней и таможенными постами, применяются межсетевые экраны. В таможне функционирует система обнаружения атак.

Обеспечение информационной безопасности в Белгородской таможне возложено на отделение информационной безопасности и технической защиты информации (далее – Отделение), которое является структурным подразделением информационно-технической службы таможни.

Отделение в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, таможенным законодательством Таможенного союза и таможенным законодательством Российской Федерации, другими федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, иными нормативными правовыми актами в области таможенного дела, Положением о Федеральной таможенной службе, нормативными и иными правовыми актами ФТС России, правовыми актами регионального таможенного управления (РТУ) и таможни, правовыми актами ФСБ России, Росинформтехнологии, правовыми актами и руководящими документами ФСТЭК России (Гостехкомиссии России), а положением об Отделении.

Организационное, методическое руководство и контроль деятельности Отделения осуществляет подразделение информационной безопасности и технической защиты информации РТУ, а в части выполнения задач и функций, возложенных на Отделение, – начальник таможни или первый

заместитель начальника таможни по таможенному контролю, начальник ИТС Белгородской таможни.

Работа Отделения строится на основе планов работы таможни, РТУ и Отделения, сочетания принципа единоначалия при решении вопросов служебной деятельности и персональной ответственности каждого должностного лица Отделения за состояние дел на порученном участке и за выполнение отдельных поручений.

Среди задач Отделения выделяются:

– осуществление в таможне и подчиненных таможенных постах единой научно-технической политики, проводимой в таможенных органах, по вопросам обеспечения информационной безопасности и технической защиты информации;

– организация и контроль эксплуатации, технического обслуживания и ремонта систем и средств защиты информации в таможне и подчиненных таможенных постах;

– защита информации в автоматизированных информационных системах и локальных сетях таможни от несанкционированного доступа;

– защита информации при подключении к открытым глобальным вычислительным сетям и при взаимодействии с внешними абонентами;

– защита информационно-вычислительных ресурсов таможни от заражения программными вирусами;

– организация эксплуатации подсистемы межсетевого экранирования;

– организация эксплуатации подсистемы криптографической защиты информации, не содержащей сведения, составляющие государственную тайну, передаваемую между таможенными органами;

– организация эксплуатации персональных средств идентификации и аутентификации в таможне;

– организация эксплуатации пункта удаленной регистрации таможни;

– контроль за соблюдением требований по защите информации от утечки информации по техническим каналам на объектах информатизации таможни и подчиненных таможенных постов.

По итогам 2017 года Отделением, в соответствии с утвержденным планом мероприятий по переводу информационных систем таможни на сертифицированные по требованиям безопасности информационные системы была произведена установка операционной системы Windows 7 на 54 автоматизированные системы доступа к сети «Интернет».

Должностными лицами Отделения реализуются следующие методы обеспечения безопасности информации при использовании сети Интернет:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов;

– использование сертифицированных средств защиты информации, обеспечивающих целостность и доступность, в том числе криптографических для подтверждения достоверности открытых и общедоступных информационных ресурсов таможенных органов (официальный сайт ФТС России, автоматизированная система таможенной статистики внешней торговли (далее - АС ТСВТ) и т.д.);

– использование электронных замков, персональных средств идентификации и аутентификации, других носителей информации для надежной идентификации, аутентификации и разграничения доступа должностных лиц таможенных органов к ресурсам сети Интернет;

– использование сертифицированных средств антивирусной защиты информации с актуальными базами антивирусных сигнатур;

– мониторинг вторжений (атак) из сети Интернет, нарушающих или создающих предпосылки к нарушению установленных требований по защите информации, и анализ защищенности, предполагающий применение специализированных программных средств (сканеров безопасности);

– контроль информации, передаваемой в сеть Интернет или загружаемой из сети Интернет;

– запрет обращения к нежелательным ресурсам в сети Интернет;

– шифрование информации при ее передаче по сети Интернет, а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации;

– сбор и анализ статистических данных о работе должностных лиц таможенных органов с ресурсами сети Интернет.

За 2017 г. выпущено 635 электронных подписей, используемых должностными лицами таможенных органов. Динамика количества выпущенных электронных цифровых подписей за 2015-2017 гг. представлено на рисунке 1.

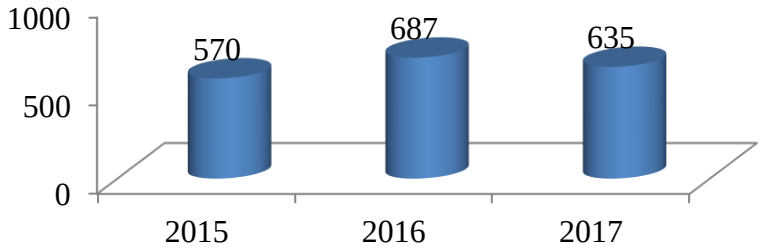

Рис. 1. Количество выпущенных электронных цифровых подписей на Белгородской таможне[1]

Постоянно осуществляется консультирование должностных лиц таможенных постов отвечающих за информационно-техническую работу по вопросам эксплуатации электронных подписей, проверки соблюдения установленных норм информационной безопасности.

Для формирования и ведения бюджетной сметы, лимитов бюджетных обязательств и управления закупками должностные лица отдела бухгалтерского учета и финансового мониторинга, и отдела тылового обеспечения были подключены к государственной интегрированной информационной системе управления общественными финансами «Электронный бюджет».

[1]Составлено по данным Отделения информационной безопасности и технической защиты информации Белгородской таможни. Документопубликован не был.

В целях совершенствования системы антивирусной защиты информации за отчетный период проводится еженедельная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях Белгородской таможни. Общее количество вирусных атак по Белгородской таможне представлено на рисунке 2.

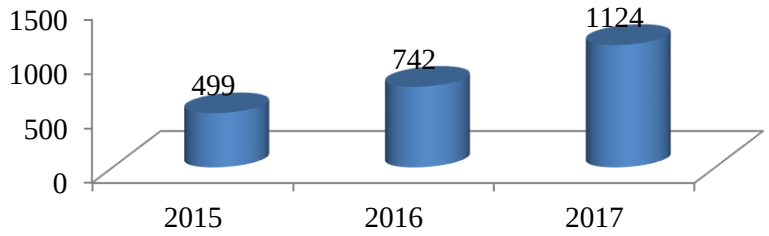

Рис. 2. Количество вирусных атак по Белгородской таможне[1]

Несмотря на достигнутые высокие результаты в обеспечении информационной безопасности в Белгородской таможне остаются нерешенными ряд задач.

В частности, такие проблемы, связанные с информатизацией как, например, «засорение виртуального пространства» и возрастание значения информационной безопасности. Развитие информационных технологий, организация информационно-правового обеспечения защиты информации в таможенном деле, объективно предполагает развитие механизмов защиты информации, обрабатываемой в автоматизированных системах.

Так же, представляется необходимым выделить таки проблемы как:

– сложность процесса межведомственного и международного обмена информацией и использование общих ресурсов;

– доступ к информации и ее защиты от информационных угроз и в связи с этим дополнительные финансовые затраты.

[1]Составлено по данным Отделения информационной безопасности и технической защиты информации Белгородской таможни. Документопубликован не был.

Возникает необходимость унификации и объединения правовых инструментов не только в рамках правового поля РФ, но и Евразийского экономического союза.

Наряду с этим стоит отметить, что в связи с развитием электронного взаимодействия всех контролирующих органов, вовлеченных в процесс перемещения товаров через таможенную границу ЕАЭС, перед таможенными органами встает необходимость обеспечения бесперебойности и надежности функционирования информационных систем с организацией многоуровневой защиты информации и каналов передачи данных

Необходимым, по нашему мнению, представляются постоянный анализ угроз информационной безопасности с точки зрения экономической эффективности, разработка методов экономической оценки информационных продуктов и услуг, выработка рекомендаций по обеспечению информационной безопасности таможенных органов. Такие проблемы можно решать с помощью научных исследований в области информатизации.

2.2. Направления совершенствования организации системы обеспечения информационной безопасности таможенных органов

Как показал проведенный анализ, обеспечение информационной безопасности в таможенных органах представляет собой сложную комплексную систему, охватывающую большой круг явлений и процессов, находящихся в стадии модернизации, связанной с активным развитием информационных систем таможни. Что, в свою очередь, требует постоянного совершенствования систем обеспечения информационной безопасности.

Среди основных направлений такого совершенствования, сегодня, можно выделить:

– формирование системы оценки угроз информационной безопасности в таможенных органах;

– обеспечение безопасности при организации международного информационного обмена;

– обеспечение защиты данных, передаваемых при межведомственном информационном обмене;

– развитие механизмов защиты информации, обрабатываемой в автоматизированных системах.

Следует отметить, что основными задачами реализации указанных направлений становятся обоснование и своевременная организация планирования мероприятий и работ по созданию новых информационно-коммуникационных технологий и их внедрение в деятельность таможенных органов, поддержание в рабочем состоянии информационно-технических средств и в актуальном состоянии используемых информационно-программных средств защиты информации.

С целью своевременного обеспечения информационной безопасности необходимо обеспечить проведение постоянного мониторинга угроз информационного обмена. Внедрение такого мониторинга позволит не только противодействовать существующим угрозам, но моделировать угрозы и оценивать риски.

Непосредственно, оценка угроз информационной безопасности будет включать в себя:

– классификацию информационных ресурсов;

– идентификацию угроз и уязвимостей, и формирование перечня источника угроз информационной безопасности;

– оценку рисков информационных угроз.

На первоначальном этапе должна быть проведена оценка критичности идентифицированности уязвимых мест и возможностей их использования для несанкционированных действий. Такая выборка позволит нам получить перечень информационных ресурсов таможенных органов, требующих защиты. Далее необходимо разбить всю защищаемую информацию на группы по уровню ценности информационных активов. Такой подход

снижает затраты на систему обеспечения информационной безопасности и, в определенной степени, упрощает документооборот в таможне. Кроме того, надо учесть, что необходимость защиты той или иной информации зависит и от длительности ее существования. С течением времени, как правило, информация перестает быть актуальной и необходимость в ее защите отпадает.

После конкретизации защищаемых информационных ресурсов необходимо идентифицировать угрозы информационной безопасности.

Построение модели угроз информационного потока в таможенных органах должно включать в себя:

– описание защищаемых информационных ресурсов;

– источники и методы реализации угроз информационной безопасности;

– уязвимость, используемых информационными источниками угроз;

– типы и масштабы возможных потерь.

С целью структурирования информационных ресурсов необходимо выстроить обобщенную структурную модель угроз информационной безопасности в ЕАИС таможенных органов. Данные следует свести в табличную форму по принципу информационный ресурс – угроза. В тех ячейках, где угроза актуальная для защищаемого объекта, должна выставляться вероятность реализации угрозы в отношении данного информационного ресурса, определенная либо экспертным путем, либо исходя из собственной статистики нарушений информационной безопасности, в противном случае выставляет нуль.

С целью проведения экспертного ранжирования угроз по их вероятности и значимости можно предложить следующую шкалу значений, представленную в таблице 2.

Оценка рисков может производиться на основании анализа количественных и качественных параметров. Качественная оценка направлена на выявление рисков и их ранжирование по вероятности и

значимости, и основывается на экспертном мнении. Количественная же оценка позволяет уточнять качественные параметры и оценить величину ущерба.

Таблица 2

Шкала значений вероятности реализации угрозы

Вероятность реализации угрозы	Описание уровня
Нереализуемая	Используемые средства защиты и методы их использования гарантируют защиту по отношению к данному типу угроз в пределах заданной уязвимости (используются сертифицированные средства защиты)
Минимальная	У источника угрозы недостаточно мотиваций или возможностей, либо существующие средства контроля способны предотвратить или, по крайней мере, значительно помешать использованию уязвимости
Средняя	Источник угрозы мотивирован и обладает возможностями, но существующие средства контроля могут препятствовать успешному использованию уязвимости
Высокая	Источник угрозы имеет высокие мотивации и достаточные возможности, а методы контроля для предотвращения проявления уязвимости не гарантируют защиту
Критическая	Уровень мотивации, технические и организационные возможности источника угроз превышают соответствующие параметры защиты

В силу труднодоступности статистических данных по угрозам информационной безопасности, оценку рисков следует проводить, основываясь на оценку экспертов.

Еще одной задачей обеспечения информационной безопасности в рамках Евразийского экономического союза является задачей обеспечения национальной безопасности страны. В настоящее время организация информационной безопасности не строится на наднациональном контроле в ЕАЭС. Каждая страна участница обеспечивает его на своей территории в соответствии со своим законодательством. В связи с этим необходимо четкое взаимодействие таможенных органов ЕАЭС для формирования единых принципов и критериев защиты информации Таможенных органов.

Для определения видов информации, являющиеся объектом потенциального нарушения информационной безопасности таможенных органов, необходимо выявить:

– цели взаимодействия;

– тип информации перемещающийся;

– порядок передачи данных.

Исходя из статьи 124 Таможенного кодекса ЕАЭС, таможенные органы используют обмен информации для задач, связанных с контролем перемещаемых товаров, соблюдением законодательства стран участниц ЕАЭС. В данной статье прописано законодательно, что обмен информацией для обеспечения таможенного контроля после выпуска товаров, является задачей всех стран. Еще одной нормативной составляющей этого процесса является соглашение о взаимной помощи между таможенными службами ЕАЭС. В данном соглашении прописан порядок и метод обмена информацией. Она осуществляется путем электронной или письменной формой передачи данных, которые формируются с помощью запросов участников Таможенного союза, либо по собственной инициативе в рамках взаимопомощи.

Также обмену подлежат документы и необходимые нормативные акты, которые требуются для производства дел. Таможенные службы стран участников ЕАЭС, вместе принимают состав данных, который необходим для информационного обмена. Кроме того, ведется работа в рамках стандартизации технических средств и порядка обмена информацией. Формируются следующие сведения для документального запроса:

– несоответствие сведений о товарах и транспортных средств;

– информация о возможном нарушении таможенного законодательства, какого-либо участника ЕАЭС;

– при применении таможенным органом, страны участника ЕАЭС, таможенного контроля.

Таможенными органами может быть сформирован запрос, не исходя из данного списка, а при наличии других законных оснований. Для получения необходимой информации таможенные органы формируют запрос в письменном виде и относят на подпись своему начальнику. Разрешается пользоваться при формировании запросов электронной почтой с защищенным каналом связи. Однако для отчетности все равно таможенным службам необходим посменный запрос, который позднее отправляется почтой.

В пункте третьем статьи 6 Соглашения о взаимной помощи подробно расписаны сведения, которые должны быть отражены в формируемом запросе. Сам запрос должен быть рассмотрен в течение одного месяца с момента его получения. Если существует необходимость более короткого срока, то участники ЕАЭС имеют право договориться о них в устном порядке. Точно также они договариваются, если срока не хватает для предоставления информации. Если таможенный орган не имеет необходимых запрашиваемому сведений, то он имеет право на их получение в соответствии со своим законодательством.

Важным моментом данной процедуры является то, что взаимодействие между таможенными службами налажено на устном уровне, что не позволяет затормозить процесс проверки.

Запрашиваемый таможенный орган в ответ на запрос, предоставляет следующие сведения:

– документы и сведения, которые были запрошены;

– данные о проведении таможенного контроля и всех необходимых мероприятий;

– любые документы и сведения, с помощью которых могут быть приняты решения запрашиваемым.

Существуют также и основания отказа таможенным органам в предоставления информации. Этот вопрос регулируется восьмой статьей соглашения о взаимной помощи. В первую очередь во внимание берут

данные, которые могут способствовать нарушению законодательства страны участника ЕАЭС.

Развитие взаимоотношений между странами участниками ЕАЭС в области обмена информацией закреплено в соглашении о требовании к обмену данными. В нем установлено, что не вся информация может подлежать обмену. Особые ограничения введены к данным, касающимся государственных тайн. К ним могут относиться любые сведения как налоговые, банковские, так и государственные. Разумеется, что информация такого рода может перемещаться, в случае гарантии запрашиваемого ее защите. Запрашиваемые таможенные органы обязуются сохранять полученные им данные, не передавать их третьим лицам, если на то не существует согласия государства, предоставившего ее в письменном виде.

В рамках взаимодействия таможенных служб ЕАЭС существует соглашение о обмене предварительной информацией. Его суть направлена на сокращения таможенных рисков в случае несоблюдения таможенного законодательства, а также унификация таможенных операций и повышение качества таможенного контроля.

Для удобства предоставления необходимых данных таможенная служба пользуется специальными техническими средствами и информационными технологиями. Это предусмотрено статьей 124 Таможенного кодекса ЕАЭС и седьмой главой Киотской конвенции, которая тоже предусматривает информационный обмен в рамках развития внешней торговли. Исходя из этих положений, комиссией ЕАЭС было принято решение о создании соглашения об обмене информацией для аналитических функций таможенных органов. Организация информационного обеспечения безопасности в рамках взаимодействия между таможенными службами ЕАЭС построена эффективным способом.

По мнению экспертов, наиболее потенциально возможными объектами таможенных правонарушений выступают, сведения таможенной статистики ЕАЭС и о применении таможенного контроля. Это наиболее, с точки зрения

угрозы обеспечения информационной безопасности таможенных органов, важные виды информации, которые могут быть объектом правонарушения. Таможенный кодекс ЕАЭС описывает порядок информационного обмена между таможенными органами иностранных государств и стран участниц ЕАЭС, тем самым давая возможность регулировать данную процедуру на национальном уровне. Способом же такого взаимодействия является заключение международных договоров.

Еще одним инструментом в обеспечении информационной целостности в процессе взаимодействия иностранных государств является представитель таможенной службы РФ за рубежом. Он необходим для эффективного осуществления международных отношений Федеральной таможенной службы России. Данные представители являются сотрудниками ФТС России. Их штатная численность за рубежом варьируется от одного человека до нескольких десятков. Это зависит в первую очередь от уровня взаимодействия иностранного государства с таможенной службой России, от значимости их интересов, а также от количества международных договоров, подписанных между двумя странами.

Таможенные представительства РФ выполняют огромный спектр задач, в том числе и обеспечение информационной безопасности таможенных органов. Основной целью считается представление национальных интересов России и исполнение поручений руководства Федеральной таможенной службы РФ.

Анализ цели организации таможенных представительств позволяет выделить ее подцели, характеристика которых позволит определить нам инструменты обеспечения информационной безопасности таможенных органов РФ.

Налаживание контактов, организация сотрудничества и взаимодействия с таможенными органами данной страны. В данном случае имеется в виду организация работы и подготовка необходимых документов и соглашений. Здесь отчетливо видно, как прорабатывается порядок передачи

информации и закрепляется в правовом и практическом поле. Представитель таможенной службы РФ налаживает связь с таможенной службой иностранного государства, договариваясь о процедуре и порядке связи, и обговаривают данные, которые будут переданы друг другу. Это очень важный момент организации взаимодействия, таможенные органы разных стран, находясь на расстоянии друг с другом, с помощью представителя Таможенной службы имеют возможность проводить связь без посредников, не боясь за сохранность информации.

Второй подцелью организации работы представителя Таможенных органов РФ является сбор и анализ актуальной информации о состоянии таможенной ситуации в данной стране. Здесь представитель таможенных органов РФ изучает имеющуюся обстановку в стране в плане правовой системы, возможного изменения законодательства. Исследуется таможенный опыт данной страны, возможности и технологии. Вся проводимая работа снабжает ФТС РФ необходимой актуальной информацией от надежного источника. Представители таможенных органов РФ проводят анализ внешнеторговых отношений между Россией и иностранной страной, выделяют возможные проблемы и пути их решений в данной области. Также он учувствует в правоохранительной работе по предотвращению нарушений таможенного законодательства двух стран, путем координации действий, курирования и мониторинга.

Представитель таможенной службы координирует деятельность участников ВЭД, активно сотрудничает с ними. При необходимости оказывает им помощь, исходя из своей компетенции. Разбираясь в сути данной подцели, можно сделать вывод, что представитель Таможенной службы РФ сильно интегрируется в деловую и административную деятельность иностранной страны. Соответственно данные представительства вынуждены адаптироваться к определенным условиям. Необходимо брать во внимание такие условия как менталитет страны, национальный язык и отличительные особенности законодательной системы.

При передаче информации из-за пределов Российской Федерации, следует учитывать: содержание информации, кем и когда передана; принцип и технологию передачи.

Одной из задач, стоящих перед таможенными органами выступает обеспечение защиты данных, передаваемых при межведомственном информационном обмене. В настоящее время государственный контроль в области таможенного дела отличается комплексным характером осуществляемых действий, главным исполнителем которого выступает ФТС России. В целях повышения эффективности своей деятельности таможенные органы осуществляют межведомственное взаимодействие с различными государственными органами исполнительной, что продиктовано сложностью регулирования общественных отношений, складывающихся в области перемещения через таможенную границу Евразийского экономического союза товаров и транспортных средств.

В современных условиях невозможно обеспечить национальную безопасность Российской Федерации в пределах ее таможенных границ без хорошо налаженного взаимодействия сил и средств государственных органов власти, координации их действий. Учитывая этот факт, таможенные органы России взаимодействуют с такими государственными органами исполнительной власти, как Федеральная налоговая служба, Пограничная служба, Федеральная служба по надзору в сфере транспорта, Федеральная служба по ветеринарному и фитосанитарному надзору, Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека и другими. Необходимость взаимодействия таможенных органов с другими ведомствами закреплена законодательством ЕАЭС. В статьях ТК ЕАЭС констатируются положения о закреплении за таможенными органами функций по координации с другими государственными органами при проведении государственного контроля, по обмену документами и информацией с использованием информационных систем и по проведению

таможенного досмотра с участием государственных органов, осуществляющих государственный контроль на таможенной границе ЕАЭС.

Необходимость взаимодействия между налоговыми и таможенными органами России обусловлена дальнейшим развитием внешнеторговой деятельности в рамках выработки согласованных позиций двух ведомств, основанных на приоритете соблюдения законных прав участников внешнеэкономической деятельности. Сотрудничество ФНС России и ФТС России основывается на обеспечении взаимного доступа к базам данных (сведений) и оперативной информации. Плановый обмен информацией в электронном виде осуществляется на федеральном уровне через Центральное информационно-техническое таможенное управление ФТС России (ЦИТТУ ФТС России) и Федеральное казенное учреждение «НалогСервис» ФНС России (ФКУ «Налог-Сервис» ФНС России).

С целью решения проблем обеспечения информационной безопасности при межведомственном взаимодействии требуется необходимо провести оценку и сопоставление процессов таможенного и налогового администрирования, анализ и доработку нормативной правовой базы ФТС и ФНС России, а также модернизировать информационные системы таможенных и налоговых служб для обеспечения их информационного взаимодействия.

При разработке технических заданий на модернизацию, должны учитываться такие принципы, как:

– исключение дублирования процедур сбора и обработки информации при соблюдении правил однократного ввода информации и обеспечение ее обработки в режиме реального времени;

– обеспечение бесперебойности и надежности функционирования информационных систем с организацией многоуровневой защиты информации и каналов передачи данных;

– обеспечение интерактивного доступа к информационным системам всех зарегистрированных пользователей вне зависимости от их территориальной удаленности от центров хранения и обработки данных.

Развитие механизмов защиты информации, обрабатываемой в автоматизированных системах, предполагает снижение технических рисков. Это достигается реализацией следующих мероприятий:

– проведение единой научно-технической политики в таможенных органах;

– организация непрерывного мониторинг отечественного рынка товаров, услуг и разработкой на основе его результатов, с учетом новейших достижений в области развития информационно-технических средств, спецификаций оборудования для размещения государственных заказов;

– использование совместимых программно-технических средств; разработкой технических требований к ИПС, создаваемым в интересах и по заказу ФТС России, с учетом их совместимости с информационными ресурсами таможенных органов;

– реализация комплекса мероприятий по обеспечению защиты информации в информационных системах таможенных органах;

– высокой технической квалификацией персонала, участвующего в подготовке документации для размещения заказов, в оценке заявок участников торгов, в испытаниях и приемке оборудования и ИПС.

Таким образом, проанализировав практику организации системы обеспечения информационной безопасности Белгородской таможни, можно сделать следующие выводы.

1. Обеспечение информационной безопасности в Белгородской таможне возложено на отделение информационной безопасности и технической защиты информации, которое является структурным подразделением информационно-технической службы таможни. Основными задачами Отделения выступают: осуществление в таможне и подчиненных таможенных постах единой научно-технической политики; организация и

контроль эксплуатации, технического обслуживания и ремонта систем и средств защиты информации в таможне и подчиненных таможенных постах; защита информации в автоматизированных информационных системах и локальных сетях таможни от несанкционированного доступа; защита информации при подключении к открытым глобальным вычислительным сетям и при взаимодействии с внешними абонентами; защита информационно-вычислительных ресурсов таможни от заражения программными вирусами и другие.

2. Среди проблем организации информационного обеспечения Белгородской таможни можно выделить: сложность процесса межведомственного и международного обмена информацией и использование общих ресурсов; необходимость обеспечения бесперебойности и надежности функционирования информационных систем с организацией многоуровневой защиты информации и каналов передачи данных в процесс перемещения товаров через таможенную границу ЕАЭС; необходимость постоянного анализа угроз информационной безопасности с точки зрения экономической эффективности, разработка методов экономической оценки информационных продуктов и услуг, выработка рекомендаций по обеспечению информационной безопасности таможенных органов.

3. Среди основных направлений совершенствования обеспечения информационной безопасности таможенных органов, сегодня, можно выделить: формирование системы оценки угроз информационной безопасности в таможенных органах; обеспечение безопасности при организации международного информационного обмена; обеспечение защиты данных, передаваемых при межведомственном информационном обмене; развитие механизмов защиты информации, обрабатываемой в автоматизированных системах.

ЗАКЛЮЧЕНИЕ

Современный этап развития характеризуется возрастанием роли информации, информационных технологий и ресурсов, что, в свою очередь, актуализирует вопросы информационной безопасности в системе обеспечения национальной безопасности государства, общества и личности. Эти вопросы напрямую касаются и таможенных органов как основного института государства, обеспечивающего его национальную безопасность в экономической сфере.

Необходимость проведения теоретических исследований по обеспечению информационной безопасности таможенных органов с организационно-правовых позиций, раскрытие роль и значимость данной деятельности, полноту ее правовой регламентации и разработки рекомендаций по повышению эффективности практической работы обусловлена особым местом организационного регулирования системе обеспечения информационной безопасности таможенных органов в системе таможенного управления, в целом.

Исследование теоретических основ организации системы обеспечения информационной безопасности таможенных органов, показало, что информационная безопасность таможенных органов представляет собой состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Обеспечение информационной безопасности призвано решать основные задачи: выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам; защита прав юридических и физических лиц на интеллектуальную собственность, а также

сбор, накопление и использование информации; защита государственной, служебной, коммерческой, личной и других видов тайн

Организация деятельности таможенных органов по обеспечению информационной безопасности осуществляется в рамках сформированного организационно-правового механизма, который представляет собой совокупность субъектов и объектов воздействия, способов, методов, мер и мероприятий, обеспечивающих состояние защищенности объектов, информации, ее свойств, инфраструктуры и т.д. Законодательство в сфере информационной безопасности таможенных органов условно можно разделить на две группы. В первую группу нормативных правовых актов, определяющую меры, направленные на соблюдение конституционных прав и свобод субъектов правоотношений в информационной сфере, развитие современных информационных и телекоммуникационных технологий, а также установление правил участия Российской Федерации в международном информационном обмене. Вторая группа представлена нормативными правовыми актами, которые закрепляют меры предупредительно-карательного характера.

Анализ практики организации системы обеспечения информационной безопасности Белгородской таможни, позволил отметить, что обеспечение возложено на отделение информационной безопасности и технической защиты информации, которое является структурным подразделением информационно-технической службы таможни. Основными задачами Отделения выступают: осуществление в таможне и подчиненных таможенных постах единой научно-технической политики; организация и контроль эксплуатации, технического обслуживания и ремонта систем и средств защиты информации в таможне и подчиненных таможенных постах; защита информации в автоматизированных информационных системах и локальных сетях таможни от несанкционированного доступа; защита информации при подключении к открытым глобальным вычислительным сетям и при взаимодействии с внешними абонентами; защита

информационно-вычислительных ресурсов таможни от заражения программными вирусами и другие.

Среди проблем организации информационного обеспечения Белгородской таможни можно выделить: сложность процесса межведомственного и международного обмена информацией и использование общих ресурсов; необходимость обеспечения бесперебойности и надежности функционирования информационных систем с организацией многоуровневой защиты информации и каналов передачи данных в процесс перемещения товаров через таможенную границу ЕАЭС; необходимость постоянного анализа угроз информационной безопасности с точки зрения экономической эффективности, разработка методов экономической оценки информационных продуктов и услуг, выработка рекомендаций по обеспечению информационной безопасности таможенных органов.

Среди основных направлений совершенствования обеспечения информационной безопасности таможенных органов, сегодня, можно выделить: формирование системы оценки угроз информационной безопасности в таможенных органах; обеспечение безопасности при организации международного информационного обмена; обеспечение защиты данных, передаваемых при межведомственном информационном обмене; развитие механизмов защиты информации, обрабатываемой в автоматизированных системах.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Таможенный кодекс Евразийского экономического союза [Электронный ресурс] (приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза) // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

2. Уголовный кодекс Российской Федерации [Текст]от 13 июня 1996 года № 63-ФЗ (ред. от 19 февраля 2018 года) // Собр. законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.

3. Кодекс Российской Федерации об административных правонарушениях [Текст]от 30 декабря 2001 года № 195-ФЗ (ред. от 07 марта 2018 года) // Собр. законодательства Рос. Федерации. – 2002. – № 1 (Ч. 1). – Ст. 1.

4. О государственной тайне[Текст] : Закон РФ от 21 июля 1993 года № 5485-1 (ред. от 26 июля 2017 года) // Собр. законодательства Рос. Федерации. -1997. – № 41. – Ст. 8220-8235.

5. О таможенном регулировании в Российской Федерации [Текст]: федер. закон от 27 ноября 2010 года № 311-ФЗ (ред. от 28 декабря 2017 года) // Собр. законодательства Рос. Федерации. – 2010. – № 48. – Ст. 6252.

6. О безопасности [Текст]: федер. закон от 28 декабря 2010 года № 390-ФЗ (ред. от 05 октября 2015 года) // Собр. законодательства Рос. Федерации. – 2011. – № 1. – Ст. 2.

7. О стратегическом планировании в Российской Федерации [Текст]: федер. закон от 28 июня 2014 года № 172-ФЗ (ред. от 31 декабря 2017 года) // Собр. законодательства Рос. Федерации. – 2014. – № 26 (часть 1). – Ст. 3378.

8. О связи [Текст]: федер. закон от 07 июля 2003 года № 126-ФЗ (ред. от 05 декабря 2017 года) // Собр. законодательства Рос. Федерации.-2003. – №28. – Ст. 2895.

9. Об информации, информационных технологиях и о защите информации [Текст]: федер. закон от 27 июля 2006 года № 149-ФЗ (ред. от 25 ноября 2017 года) // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3448.

10. О персональных данных [Текст]: федер. закон от 27 июля 2006 года № 152-ФЗ (ред. от 29 июля 2017 года) // Собр. законодательства Рос. Федерации. – 2006. – № 31. – Ст. 3451.

11. О коммерческой тайне [Текст]: федер. закон от 29 июля 2004 года № 98-ФЗ (ред. от 12 марта 2014 года) // Собр. законодательства Рос. Федерации. – 2004. – № 32. – Ст. 3283.

12. Об утверждении Доктрины информационной безопасности Российской Федерации [Текст]: Указ президента РФ от 05 декабря 2016 года № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.

13. О Стратегии развития таможенной службы Российской Федерации до 2020 года [Текст]: Распоряжение правительства РФ от 28 декабря 2012 года № 2575-р // Собр. законодательства Рос. Федерации. – 2013. – № 2. – Ст. 109.

14. Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года [Электронный ресурс]: Приказ ФТС России от 13 декабря 2010 года № 2401. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

15. Об утверждении Положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации [Электронный ресурс]: Приказ ФТС РФ от 07 октября 2010 года № 1866 // Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

16. Об утверждении Положения и состава Совета по обеспечению информационной безопасности таможенных органов Российской Федерации [Электронный ресурс]: Приказ ФТС России от 22 августа 2011 года № 1702 //

Справочно-правовая система «КонсультантПлюс». Информ. банк. «Версия Проф». Разд. «Законодательство».

17. Абрамов, А. С. Перспективы совершения таможенных операций в свете развития ЕАИС таможенных органов [Текст] / А. С. Абрамов // Управленческое консультирование. – 2017. – № 6 (102). – С. 16-21.

18. Аксенов, И. А. Информационная безопасность таможенных органов Российской Федерации и Евразийского экономического союза [Текст] / И. А. Аксенов // Инновационное развитие экономики. – 2018. – № 1 (143).– С. 357-361.

19. Алексеева, Л. Н. Система информационной безопасности органов государственной власти как основа современного государственного управления [Текст] / Л. Н. Алексеева // Вестник Университета (Государственный университет управления). – 2015. – № 13. – С. 5-9.

20. Барбышева, Г. И. Обеспечение информационной безопасности таможенных органов РФ [Текст] : материалы II Международной научной конференции «Инновационная экономика» / Г. И. Барбышева, Ш. Ф. Мирзаев. – Казань : Изд-во «Бук», 2015. – С. 22-24.

21. Башлы, П. Н. Актуальные проблемы информационной безопасности в таможенных органах Российской Федерации [Текст] : материалы научно-практической конференции: в 2 частях «Особенности государственного регулирования внешнеторговой деятельности в современных условиях» / П. Н. Башлы. – Р-на-Д : Российская таможенная академия, Ростовский филиал, 2015. – С. 30-35.

22. Белгородская таможня подводит итоги [Электронный ресурс]. Сайт ФТС России. – Режим доступа:http://ctu.customs.ru/index.php?option=com_content&view=article&id=16113:2017-12-22-06-09-57&catid=103:info-o-tek-deyat-bel-cat&Itemid=145.

23. Бормотова, Е. Г. Межведомственное информационное взаимодействие для обеспечения выполнения контрольных функций таможенными органами [Текст] : монография / Е. Г. Бормотова,

Н. Г. Липатова. – М. : Изд-во Российской таможенной академии, 2014. – 218 с.

24. Бурькова, Е. В. Задача обеспечения информационной безопасности таможенных органов [Текст] : материалы XI Всероссийской научно-практической конференции «Современные информационные технологии в науке, образовании и практике» / Е. В. Бурькова, А. В. Маслова. – Оренбург : Изд-во Оренбургского государственного университета, 2014. – С. 114-119.

25. Вагина, А. В. Обеспечение экономической безопасности во внешнеторговой сфере Российской Федерации [Текст] : материалы VI международной научной конференции «Проблемы современной экономики» / А. В. Вагина. – Самара : Изд-во «АСГАРД», 2017. – С. 117-122.

26. Ведерников, А. Е. Актуальные проблемы обеспечения информационной безопасности в органах государственного управления [Текст] : сб. «Актуальные вопросы обеспечения информационной безопасности» / А. Е. Ведерников. – Белгород : Белгородский университет кооперации, экономики и права, 2015. – С. 50-54.

27. Власенков, Г. Ю. Информационная безопасность таможенных технологий [Текст] : монография / Г. Ю. Власенков, В. А. Карданов. – М. : изд-во Юстиция, 2016. – 70 с.

28. Воронов, А. М. Содержание правового института «информационная безопасность таможенной деятельности» [Текст] / А. М. Воронов, Н. М. Кожуханов // Финансы: теория и практика. – 2013. – № 4 (76). – С. 81-89.

29. Клименко, С. Н. Информационная безопасность таможенных органов: актуальные направления совершенствования административно-правового обеспечения [Текст] / С. Н. Клименко // Ученые записки Санкт-Петербургского имени В.Б. Бобкова филиала Российской таможенной академии. – 2016. – № 3 (59). – С. 44-48.

30. Клименко, С. Н. Правовые основы информационной безопасности в таможенных органах Российской Федерации [Текст] : монография / С. Н. Клименко. – СПб. : Санкт-Петербургский имени В.Б. Бобкова филиал Российской таможенной академии, 2013. – 100 с.

31. Кожуханов, Н. М. Модель обеспечения информационной безопасности таможенной деятельности [Текст] : монография / Н. М. Кожуханов. – М. : Изд-во Российской таможенной академии, 2012. – 119 с.

32. Кожуханов, Н. М. Направления обеспечения информационной безопасности таможенных органов [Текст] : материалы VI Международной молодежной научно-практической конференции «Основные направления развития таможенного дела в условиях членства России во всемирной торговой организации» / Н. М. Кожуханов. – М. : Изд-во Российской таможенной академии, 2014. – С. 110-115.

33. Коренькова, В. И. Обеспечение информационной безопасности: таможенный аспект [Текст] / В. И. Коренькова // Ростовский научный журнал. – 2017. – № 1. – С. 234-240.

34. Крайдуба, Е. Ю. Проблемы обеспечения информационной безопасности в таможенных органах Российской Федерации [Текст] : сб. статей международной научно-практической конференции в 3-х частях «Научные революции: сущность и роль в развитии науки и техники» / Е. Ю. Крайдуба. – Уфа : Изд-во Общество с ограниченной ответственностью «Аэтерна», 2017. – С. 114-116.

35. Купрюхина, Л. И. Культура информационной безопасности в органах государственной власти [Текст] / Л. И. Купрюхина // Инновации в гражданской авиации. – 2016. – № 1. – С. 83-88.

36. Медовкина, Л. Ю. Эффективность деятельности государственных органов в сфере обеспечения информационной безопасности [Текст] : материалы II Международной научно-практической конференции «Государственная политика: методология, практика, направления совершенствования» / Под редакцией П.А. Меркулова / Л. Ю. Медовкина. –

Орел : Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации. Орловский филиал, 2017. – С. 89-92.

37. Мильшина, И. В. Информационное обеспечение деятельности таможенных органов: вопросы безопасности [Текст] / И. В. Мильшина, А. О. Медведева // Информационная безопасность регионов. – 2013. – № 1 (12). – С. 46-50.

38. Морозов, А. В. Организационно-правовое обеспечение информационной безопасности [Текст] : монография / А. В. Морозов, Т. А. Полякова –М. : РПА Минюста России, 2013. – 276 с.

39. Мошкина, Н. А. Обеспечение информационной безопасности таможенных органов на современном этапе [Текст] : материалы III всероссийской научно-практической конференции: в 2 частях «Особенности государственного регулирования внешнеторговой деятельности в современных условиях» / Н. А. Мошкина. – Р-на-Д : Российская таможенная академия, Ростовский филиал, 2016. – С. 186-191.

40. Недосекова, Е. С. Административно-правовой механизм обеспечения информационной безопасности таможенных органов Российской Федерации [Текст] : монография / Е. С. Недосекова. – М. : Изд-во Российской таможенной академии, 2013. – 119 с.

41. Никитин, Б. Г. Информационная безопасность таможенных органов Российской Федерации в контексте интеграционных процессов [Текст] / Б. Г. Никитин // Академический вестник Ростовского филиала Российской таможенной академии. – 2016. – № 2 (23). – С. 27-31.

42. Общая информация о Белгородской таможне [Электронный ресурс]. Сайт ФТС России. – Режим доступа: http://ctu.customs.ru/.

43. Основные итоги деятельности Белгородской таможни за 1 квартал 2018 года [Электронный ресурс]. Сайт ФТС России. – Режим доступа:

http://ctu.customs.ru/index.php?option=com_content&view=article&id=17016:-1-2018-&catid=103:info-o-tek-deyat-bel-cat&Itemid=145.

44. Растрыгина, К. С. Совершенствование системы информационной безопасности в органах государственной власти [Текст] :сб. статей IX международной научно-практической конференции «EurasiaScience» / К. С. Растрыгина. – М. : Изд-во: Общество с ограниченной ответственностью «Актуальность.РФ», 2017. – С. 304-306.

45. Саенко, В. В. Основные направления развития информационно-коммуникационных технологий в таможенных органах Российской Федерации [Текст] / В. В. Саенко, С. А. Куштапин, В. В. Гарбуз, В. В. Черных, Е. В. Зыбина // Транспортное дело России. – 2015. – № 3. – С. 111-116.

46. Сведения о государственных информационных системах, находящихся в ведении Белгородской таможни [Электронный ресурс]. Сайт ФТС России. –Режим доступа: http://ctu.customs.ru/index.php?option=com_content&view=article&id=437:sved-o-gos-inf-sis-bel&catid=121:info-o-gos-bel-cat&Itemid=163.

47. Сомов, Ю. И. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов [Текст] : монография / Ю.И. Сомов, Э.П. Купринов, С.В. Курихин, Л.Д. Зайцева. – М. : Изд-во Российской таможенной академии, 2014. – 186 с.

48. Тарарышкин, Ю. В. Информационные технологии – инструмент управления внешнеторговыми операциями [Текст] :материалы IV Международной научно-практической конференции «Информационные технологии в экономике, бизнесе и управлении» / Ю. В. Тарарышкин. – Тамбов : Тамбовский государственный университет имени Г.Р. Державин, 2017. – С. 217-225.

49. Усков, А. В. Информационные таможенные технологии [Текст] / А. В. Усков, О. В. Ясенев. – Нижний Новгород : Нижегородский госуниверситет им. Н.И. Лобачевского, 2014 – 60 с.

50. Филяк, П. Ю. Обеспечение информационной безопасности в органах государственной власти на основе качественного подхода к анализу рисков [Текст] : сб. международной научно-практической конференции «Современные проблемы и задачи обеспечения информационной безопасности (СИБ - 2015)» / П. Ю. Филяк, А. В. Русанов. – М. : Изд-во Московского финансово-юридического университета МФЮА, 2015. – С. 41-46.

51. Хлыстова, П. Н. Совершенствование методов обеспечения информационной безопасности в таможенном деле [Текст] : сб. научных статей V Всероссийской междисциплинарной молодежной научной конференции «Проблемы правовой и технической защиты информации сборник» / П. Н. Хлыстова. – Барнаул : Изд-во ФГБОУ ВПО «Алтайский государственный университет», 2017. – С. 115-122.

52. Чеботарева, А. А. К вопросу о проблемах обеспечения информационной безопасности в таможенных органах [Текст] / А. А. Чеботарева // Таможенное дело. – 2012. – № 2. – С. 11-15.

53. Шавшина, С. А. Применение информационных технологий в таможенной сфере и анализ проблем информационной безопасности [Текст] : сб. трудов конференции «Тенденции инновационных процессов в науке» / С. А. Шавшина, П. А. Нуратинова. – М. : Изд-во ООО «Европейский фонд инновационного развития», 2015. – С. 83-86.

54. Шубин, П. С. Информационная безопасность органов государственной власти [Текст] : сб. статей международной научно-практической конференции: в 3 частях «Информация как двигатель научного прогресса» / П. С. Шубин. – Екатеринбург : Изд-во НИЦ «Аэтерна», 2017. – С. 91-96.